IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of	:	THE COMMISSIONER IS AUTHORIZED TO CHARGE ANY DEFICIENCY IN THE FEES FOR THIS PAPER TO DEPOSIT ACCOUNT NO. 23-0975
Masaki YAMAUCHI et al.	:	
Serial No. NEW	:	**Attn: APPLICATION BRANCH**
Filed July 29, 2003	:	Attorney Docket No. 2003_1057A

AUTHENTICATION APPARATUS
AND AUTHENTICATION METHOD

CLAIM OF PRIORITY UNDER 35 USC 119

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

Applicants in the above-entitled application hereby claim the date of priority under the International Convention of Japanese Patent Application No. 2002-226532, filed August 2, 2002, as acknowledged in the Declaration of this application.

A certified copy of said Japanese Patent Application is submitted herewith.

Respectfully submitted,

Masaki YAMAUCHI et al.

By _____
W. Douglas Hahm
Registration No. 44,142 *for*
Michael S. Huppert
Registration No. 40,268
Attorney for Applicants

MSH/kjf
Washington, D.C. 20006-1021
Telephone (202) 721-8200
Facsimile (202) 721-8250
July 29, 2003

日　本　国　特　許　庁
JAPAN　PATENT　OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出願年月日
Date of Application:　２００２年　８月　２日

出願番号
Application Number:　特願２００２－２２６５３２

[ST.10/C]:　[ＪＰ２００２－２２６５３２]

出願人
Applicant(s):　松下電器産業株式会社

２００３年　３月１４日

特許庁長官
Commissioner,
Japan Patent Office　太田信一郎

出証番号　出証特２００３－３０１７２８４

【書類名】　特許願

【整理番号】　2022540089

【あて先】　特許庁長官殿

【国際特許分類】　H04Q　7/34

G01C 21/00

【発明者】

【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内

【氏名】　山内　真樹

【発明者】

【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内

【氏名】　岡林　一郎

【発明者】

【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内

【氏名】　森　康浩

【発明者】

【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内

【氏名】　川端　章裕

【発明者】

【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内

【氏名】　余田　貞人

【特許出願人】

【識別番号】　000005821

【氏名又は名称】　松下電器産業株式会社

【代理人】

【識別番号】　100109210

【弁理士】

【氏名又は名称】　新居　広守

【電話番号】　06-4806-7530

【手数料の表示】

【予納台帳番号】　049515

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　認証装置及び認証方法

【特許請求の範囲】

【請求項１】　特定の個体を対象として、その正当性を認証する認証装置であって、

前記個体から、当該個体を特徴づける第１対象情報を取得する対象情報取得手段と、

前記取得された第１対象情報に基づいて、前記個体の正当性を認証する対象情報認証手段と、

前記正当性が認証された個体が存在する位置を表わす位置情報を取得して前記対象情報に対応づける位置情報付加手段と

を備えることを特徴とする認証装置。

【請求項２】　前記認証装置は、さらに、

前記特定の個体を認識するための第２対象情報を予め記憶している記憶手段を備え、

前記対象情報認証手段は、

前記記憶手段から、前記特定の個体に係る第２対象情報を読み出し、当該第２対象情報と前記取得された第１対象情報とを照合し、その結果が一致した場合に、前記特定の個体が正当であると認証する

ことを特徴とする請求項１記載の認証装置。

【請求項３】　前記特定の個体は、特定の個人である

ことを特徴とする請求項１又は２記載の認証装置。

【請求項４】　前記対象情報取得手段は、

前記第１対象情報として、前記特定の個人を識別し得るパスワード、指紋、声紋、顔の外観及び虹彩を表わす対象情報のうち、少なくとも一の情報を取得し、

前記対象情報認証手段は、

前記取得された第１対象情報に基づいて、前記認証を行なう

ことを特徴とする請求項３記載の認証装置。

【請求項５】　前記特定の個体は、特定の個人及び当該個人が所持する物品

である

ことを特徴とする請求項１又は２記載の認証装置。

【請求項６】　前記対象情報取得手段は、

前記第１対象情報として、前記特定の個人を識別し得るパスワード、指紋、声紋、顔の外観及び虹彩を表わす対象情報のうち、少なくとも一の情報を取得し、かつ前記物品を特徴付ける識別コード及び当該物品の外観を表わす対象情報のうち、少なくとも一の対象情報を取得し、

前記対象情報認証手段は、

前記取得された第１対象情報に基づいて、重畳して前記認証を行なう

ことを特徴とする請求項５記載の認証装置。

【請求項７】　前記位置情報付加手段は、

ＧＰＳ（Global Positioning System）によって、前記個体が存在する位置の位置情報を取得する

ことを特徴とする請求項１又は２記載の認証装置。

【請求項８】　前記位置情報付加手段は、ＰＨＳ（Personal Handyphone System）又は携帯電話システムの基地局から、前記個体が存在する位置の位置情報を取得する

ことを特徴とする請求項１又は２記載の認証装置。

【請求項９】　前記認証装置は、さらに、年月日字分秒を計時し得る時計を内蔵し、

前記位置情報付加手段は、さらに、

前記時計から前記個体が存在する時刻を表わす時間情報を取得して付加する

ことを特徴とする請求項１～８項の何れか１項に記載の認証装置。

【請求項１０】　前記位置情報付加手段は、さらに、

電波時計システムから前記個体が存在する時刻を表わす時間情報を取得して付加する

ことを特徴とする請求項１～８項の何れか１項に記載の認証装置。

【請求項１１】　特定の個体を対象として、その正当性と当該個体が実存することを認証する認証装置であって、

前記個体を特徴づける対象情報を取得する対象情報取得手段と、

前記個体が存在する位置を表わす位置情報を取得する位置情報取得手段と、

前記取得された対象情報に基づいて、前記個体の正当性を認証する対象情報認証手段と、

前記取得された位置情報に基づいて、前記個体が存在する位置を認証する位置情報認証手段と、

前記個体の正当性が認証され、前記位置情報が認証された場合に、前記個体が実存すると認証する実存認証手段と

を備えることを特徴とする認証装置。

【請求項１２】　前記認証装置は、さらに、

前記特定の個体を認識するための第２対象情報を予め記憶している記憶手段を備え、

前記対象情報認証手段は、

前記記憶手段から、前記特定の個体に係る第２対象情報を読み出し、当該第２対象情報と前記取得された第１対象情報とを照合し、その結果が一致した場合に、前記特定の個体が正当であると認証する

ことを特徴とする請求項１１記載の認証装置。

【請求項１３】　前記特定の個体は、特定の個人及び当該個人が所持する物品である

ことを特徴とする請求項１１又は１２記載の認証装置。

【請求項１４】　前記対象情報取得手段は、

前記特定の個人を識別し得るパスワード、指紋、声紋、顔の外観及び虹彩を表わす対象情報のうち、少なくとも一の対象情報を取得し、かつ前記物品を識別し得る識別コード及び当該物品の外観を表わす対象情報を取得し、

前記対象情報認証手段は、

前記取得された対象情報に基づいて、重畳して前記認証を行なう

ことを特徴とする請求項１３記載の認証装置。

【請求項１５】　前記位置情報取得手段は、

ＧＰＳ（Global Positioning System）によって、前記個体が存在する位置の

位置情報を取得する

ことを特徴とする請求項１１又は１２記載の認証装置。

【請求項１６】　前記位置情報取得手段は、

ＰＨＳ（Personal Handyphone System）又は携帯電話システムの基地局から、前記個体が存在する位置の位置情報を取得する

ことを特徴とする請求項１１又は１２記載の認証装置。

【請求項１７】　前記認証装置は、さらに、

前記個体が存在した時刻を表わす時間情報を取得する時間情報取得手段と、

前記取得された時間情報に基づいて、前記個体が存在した時刻を認証する時間情報認証手段とを備え、

前記実存認証手段は、さらに、

前記認証された時刻において前記個体が実存すると認証する

ことを特徴とする請求項１５又は１６項に記載の認証装置。

【請求項１８】　前記認証装置は、さらに、年月日字分秒を計時し得る時計を内蔵し、

前記時間情報認証手段は、さらに、

前記内蔵する時計から前記個体が存在する時刻を表わす時間情報を取得して認証する

ことを特徴とする請求項１７記載の認証装置。

【請求項１９】　前記時間情報認証手段は、さらに、

電波時計システムから前記個体が存在する時刻を表わす時間情報を取得して認証する

ことを特徴とする請求項１７記載の認証装置。

【請求項２０】　前記認証装置は、さらに、

前記特定の個体を特徴づける対象情報と、当該個体が所定の予定に従って移動された場合における移動後の位置及び時刻を表わす位置情報及び時間情報とを予め記憶する記憶手段を備え、

前記対象情報認証手段は、

前記記憶手段から、前記特定の個体に係る対象情報を読み出し、当該読み出さ

れた対象情報と前記取得された対象情報とを照合し、その結果が一致した場合に、前記特定の個体が正当であると認証し、

前記位置情報認証手段は、

前記記憶手段から、前記特定の個体に係る前記移動後の位置情報を読み出し、当該読み出された位置情報と前記取得された位置情報とを照合し、その結果が一致した場合に、前記特定の個体が存在する位置が正当であると認証し、

前記時間情報認証手段は、

前記記憶手段から、前記特定の個体に係る前記移動後の時間情報を読み出し、当該読み出された時間情報と前記取得された時間情報とを比較し、それらが同じ時間帯であると判定された場合に、前記特定の個体が存在する時刻が正当であると認証する

ことを特徴とする請求項１８又は１９記載の認証装置。

【請求項２１】　特定の個人及び当該個人が所持する特定の物品のうち、少なくとも一つの個体を対象として、当該個体の正当性と当該個体が実存することを認証するための認証サーバと、当該認証サーバにネットワークを介して接続されている認証用端末とからなる認証システムであって、

前記認証用端末は、

前記個体から、当該個体を特徴づける対象情報を取得する対象情報取得手段と、

前記個体が存在する位置を表わす位置情報を取得する位置情報取得手段と、

取得された前記対象情報及び前記位置情報を前記認証サーバに送信する送信手段とを備え、

前記認証サーバは、

前記認証用端末から対象情報及び位置情報とを受信する受信手段と、

前記受信された対象情報に基づいて、前記個体の正当性を認証する対象情報認証手段と、

前記受信された位置情報に基づいて、前記個体が存在する位置を認証する位置情報認証手段と、

前記個体の正当性が認証され、前記位置情報が認証された場合に、前記個体が

実存すると認証する実存認証手段とを備える

ことを特徴とする認証システム。

【請求項２２】　前記認証用端末の前記対象情報取得手段は、

前記特定の個人を識別し得るパスワード、指紋、声紋、顔の外観及び虹彩を表わす対象情報のうち、少なくとも一の対象情報を取得し、前記物品を識別し得る識別コード及び当該物品の外観を表わす対象情報のうち、少なくとも一の対象情報を取得し、

前記認証サーバの前記対象情報認証手段は、

前記受信された対象情報に基づいて、重畳して前記認証を行なう

ことを特徴とする請求項２１記載の認証システム。

【請求項２３】　前記認証用端末の前記位置情報取得手段は、

ＧＰＳ（Global Positioning System）によって、前記個体が存在する位置の位置情報を取得する

ことを特徴とする請求項２１記載の認証システム。

【請求項２４】　前記認証用端末の前記位置情報取得手段は、

ＰＨＳ（Personal Handyphone System）又は携帯電話システムの基地局から、前記個体が存在する位置の位置情報を取得する

ことを特徴とする請求項２１記載の認証システム。

【請求項２５】　前記認証用端末は、さらに、

前記個体が存在した時刻を表わす時間情報を取得する時間情報取得手段を備え、

前記送信手段は、前記取得された時間情報をも前記認証サーバに送信し、

前記認証サーバの前記受信手段は、さらに、前記認証用端末から時間情報を受信し、

前記認証サーバは、さらに、

受信された前記時間情報に基づいて、前記個体が存在した時刻を認証する時間情報認証手段とを備え、

前記実存認証手段は、さらに、

前記認証された時刻において前記個体が実存すると認証する

ことを特徴とする請求項２３又は２４記載の認証システム。

【請求項２６】　前記認証サーバは、さらに、年月日字分秒を計時し得る時計を内蔵し、

前記時間情報認証手段は、さらに、

前記内蔵する時計から前記個体が存在する時刻を表わす時間情報を取得して認証する

ことを特徴とする請求項２５記載の認証システム。

【請求項２７】　前記認証サーバの前記時間情報認証手段は、さらに、

電波時計システムから前記個体が存在する時刻を表わす時間情報を取得して認証する

ことを特徴とする請求項２５記載の認証システム。

【請求項２８】　前記認証サーバは、さらに、

前記特定の個体を特徴づける対象情報と、当該個体が所定の予定に従って移動された場合における移動後の位置及び時刻を表わす位置情報及び時間情報とを予め記憶する記憶手段を備え、

前記認証サーバにおいて、

前記対象情報認証手段は、

前記記憶手段から、前記特定の個体に係る対象情報を読み出し、当該読み出された対象情報と前記受信された対象情報とを照合し、その結果が一致した場合に、前記特定の個体が正当であると認証し、

前記位置情報認証手段は、

前記記憶手段から、前記特定の個体に係る前記移動後の位置情報を読み出し、当該読み出された位置情報と前記受信された位置情報とを照合し、その結果が一致した場合に、前記特定の個体が存在する位置が正当であると認証し、

前記時間情報認証手段は、

前記記憶手段から、前記特定の個体に係る前記移動後の時間情報を読み出し、当該読み出された時間情報と前記受信された時間情報とを比較し、それらが同じ時間帯であると判定された場合に、前記特定の個体が存在する時刻が正当であると認証する

ことを特徴とする請求項２６又は２７記載の認証装置。

【請求項２９】　前記認証用端末の送信手段は、さらに、

認証用端末を識別し得る情報を、前記対象情報及び前記位置情報に付加して前記認証サーバに送信し、

前記認証サーバの受信手段は、さらに、

前記受信した認証用端末を識別し得る情報が正当か否かを判別し、正当な情報であると判別された場合に、前記受信した対象情報及び位置情報を有効な情報として扱う

ことを特徴とする請求項２８記載の認証システム。

【請求項３０】　前記認証サーバは、さらに、

前記受信した認証用端末を識別し得る情報が正当な情報でないと判別された場合に、当該認証用端末に所定の警告を表わす情報を送信する警告送信手段を備え、

前記認証用端末は、さらに、

前記認証サーバから、前記警告を表わす情報を受信し、当該情報の内容を提示する警告受信手段を備える

ことを特徴とする請求項２９記載の認証システム。

【請求項３１】　前記認証用端末の送信手段は、さらに、

前記対象情報及び前記位置情報を暗号化して前記認証サーバに送信し、

前記認証サーバの受信手段は、さらに、

前記認証用端末から受信した暗号化された対象情報及び位置情報を復号する

ことを特徴とする請求項２９記載の認証システム。

【請求項３２】　前記認証サーバは、さらに、

所定の規則に基づいて、前記認証用端末を識別し得る情報を更新して前記認証用端末に通知し、

前記認証用端末は、さらに、

所定の規則に基づいて、前記認証サーバから通知により、前記認証用端末を識別し得る情報を更新する

ことを特徴とする請求項２９記載の認証システム。

【請求項３３】　特定の作業員の正当性と当該作業員が存在する位置を把握して所定の施設における施錠を管理する管理サーバと、当該管理サーバにネットワークを介して接続されている作業員端末とからなる施錠管理システムであって、

前記作業員端末は、

前記作業員から、当該作業員を特徴づける対象情報を取得する対象情報取得手段と、

前記作業員が存在する位置を表わす位置情報を取得する位置情報取得手段と、

取得された前記対象情報及び前記位置情報を前記管理サーバに送信する送信手段とを備え、

前記管理サーバは、

前記作業員端末から対象情報及び位置情報とを受信する受信手段と、

前記受信された対象情報に基づいて、前記作業員の正当性を認証する対象情報認証手段と、

前記受信された位置情報に基づいて、前記作業員が存在する位置が安全な位置か否かを判別する位置情報判別手段と、

前記作業員の正当性が認証され、前記作業員の位置が安全な位置であると判別された場合に、前記所定の施設に施錠を行なう

ことを特徴とする施錠管理システム。

【請求項３４】　特定の社員の正当性と当該社員が存在する位置と時刻とを把握して所定の訪問先に対する巡回訪問を管理する管理サーバと、当該管理サーバにネットワークを介して接続されている社員端末とからなる巡回管理システムであって、

前記社員端末は、

前記社員から、当該社員を特徴づける対象情報を取得する対象情報取得手段と、

前記社員が存在する位置を表わす位置情報を取得する位置情報取得手段と、

前記社員が存在する時刻を表わす時間情報を取得する時間情報取得手段と、

取得された前記対象情報、前記位置情報及び前記時間情報を前記管理サーバに

送信する送信手段とを備え、

前記管理サーバは、

前記社員端末から前記対象情報、前記位置情報及び前記時間情報とを受信する受信手段と、

前記受信された対象情報に基づいて、前記社員の正当性を認証する対象情報認証手段と、

前記受信された位置情報に基づいて、前記社員が存在する位置が正当な訪問先の位置か否かを判別する位置情報判別手段と、

前記受信された時間情報に基づいて、前記社員が存在する時刻が正当な時間か否かを判別する時間情報判別手段と、

前記社員の正当性が認証され、前記社員の位置及び時間が正当な位置及び時間であると判別された場合に、前記巡回訪問は正当であると判定する

ことを特徴とする巡回管理システム。

【請求項３５】　特定の個体を対象として、その正当性を認証する認証方法であって、

前記個体から、当該個体を特徴づける第１対象情報を取得する対象情報取得ステップと、

前記取得された対象情報に基づいて、前記個体の正当性を認証する対象情報認証ステップと、

前記正当性が認証された個体が存在する位置を表わす位置情報を取得して前記対象情報に対応づける位置情報付加ステップと

を有することを特徴とする認証方法。

【請求項３６】　特定の個体を対象として、その正当性と当該個体が実存することを認証する認証方法であって、

前記個体を特徴づける対象情報を取得する対象情報取得ステップと、

前記個体が存在する位置を表わす位置情報を取得する位置情報取得ステップと、

前記取得された対象情報に基づいて、前記個体の正当性を認証する対象情報認証ステップと、

前記取得された位置情報に基づいて、前記個体が存在する位置を認証する位置情報認証ステップと、

前記個体の正当性が認証され、前記位置情報が認証された場合に、前記個体が実存すると認証する実存認証ステップと

を有することを特徴とする認証方法。

【請求項３７】　特定の個体を対象として、その正当性を認証する認証装置のためのプログラムであって、

請求項３５記載の認証方法に含まれる全てのステップをコンピュータに実行させることを特徴とするプログラム。

【請求項３８】　特定の個体を対象として、その正当性と当該個体が実存することを認証する認証装置のためのプログラムであって、

請求項３６記載の認証方法に含まれる全てのステップをコンピュータに実行させることを特徴とするプログラム。

【発明の詳細な説明】

【発明の属する技術分野】

本発明は、特定の個人や特定の物品を対象とする認証装置に関する。特に、それらの対象が、特定の位置や特定の時間に存在する場合についても認証し得る認証装置に関する。

【０００１】

【従来の技術】

従来、「特定の位置」に「特定の個体（人や物）」が「存在すること／存在したこと」を管理したい場合がある。例えば、営業マンの外回りの活動をその上司が管理する「巡回管理」が該当する。この場合、従来の技術では、ＧＰＳ端末や携帯電話等を営業マンに携帯させ、ＧＰＳや携帯電話の基地局から送信される位置情報等に基づいて「位置追跡」や「位置特定」を行ない、その位置情報等を上司が使用する管理サーバに送信させることによって、上記の管理を行なっている。

【０００２】

また、例えば、特開２０００－２０９６４１号公報記載の「位置情報通信シス

テム」（従来例１）や、特表２００１－５０３１３４号公報記載の「地理データマネージャ」（従来例２）や、特開２００１－９１２９１号公報記載の「情報処理装置」（従来例３）や、特開２０００－３５４２６８号公報記載の「ロケーション管理システム」（従来例４）等の場合は、所定の端末の位置情報に基づいて位置の確認／特定が可能である。さらに、特開２０００－１９７０９８号公報記載の「位置情報管理装置」（従来例５）は、位置情報の通知機能を有する端末同士での位置情報の共有が可能である。さらにまた、特開２０００－３０４５６４号公報記載の「探索用携帯端末機」（従来例６）は、特定の個人（徘徊者）の位置情報を入手することができる。

【０００３】

さらに、特開２００１－１１９７６１に記載の「情報提供システム」（従来例７）は、端末利用者が所定の場所に行ったときにその利用者が予め要求していた情報を得ることができる。さらに、特開２００１－３６８４０号公報記載の「撮影画像管理方法」（従来例８）は、デジタルカメラで撮影された画像にその撮像場所情報を添付することができる。

なお、上記の声紋データを用いる認証方法については、特開平８－２２３２８１「携帯電話機」等に記載されている。また、顔の特徴を表わした画像データを用いる認証方法については、特開平１１－８５９８８「顔画像認識システム」等に記載されている。さらにまた、虹彩データを用いる認証方法については、特開平９－２１２６４４「虹彩認識装置及び虹彩認識方法」等に記載されている。

【０００４】

【発明が解決しようとする課題】

しかしながら、これらの従来例は、特定の人物に１対１に対応して装置が与えられ、その装置に位置情報を送信することが絶対条件となっている。そのため、「特定の人物以外によって端末が特定の位置まで運ばれた場合」といった「なりすまし」的ケースに対して全く無力である。

また、「特定の位置（場所）」に「特定の個体」が存在すること（存在したこと）を認識したい状況において、「特定の個体」が認識したい側からみて「不特定多数」である場合にも無力である。つまり、特定の個体と従来の機器が１対１

に対応していない場合、従来の機器では認証そのものが不可能である。言い換えると、「位置（場所）」と「個体」の双方を認証できる端末装置、もしくは端末装置とサーバ装置からなるシステムが存在していないために、これらの問題が起こっている。

【０００５】

具体的には、以下に示す各状況に対して有効に機能できる技術が存在しない。

（１）「特定の物品」が「特定の位置」存在すること、又は「特定の個人」と「特定の物品」とを認証したい状況（特定の住所に対する配達の認証、物品受け渡しの認証など）

（２）「特定の位置」に「特定の人物」が存在することを認証したい状況（営業マンの巡回管理、オリエンテーリング状況管理など）

（３）個体（例えば、個人や物品等）の「特定の行動や移動」を認証したい状況（出張管理、産業廃棄物の廃棄管理、撮影データや録音データ等の著作証明など）

（４）一つ以上の「個体とその位置の認証」により、新たな２次的効果を得たい状況（特定の施設に対するリモート施錠管理など）

【０００６】

なお、上記従来例１～従来例５においては、個人を特定し、その認証を行なうことは不可能である。また、従来例６や従来例７では、いわゆる「なりすまし」には対応できないため、提供される情報は、なりすました偽利用者に筒抜けとなる。例えば、上記のリモート施錠管理の場合であれば鍵が開いてしまう。

さらに、従来例８は、撮影者情報を添付することはできない。仮に、そのような装置を付け加えることによって画像データに撮像場所情報と撮影者情報を添付したとしても、容易に改変できるため、認証装置として機能し得ない。

そこで、本発明は、上記課題に鑑みてなされたものであり、特定の個人や特定の物品の存在の正当性について、確度の高い認証装置を提供することを目的とする。

【０００７】

【課題を解決するための手段】

上記目的を達成するために、本発明に係る認証装置は、特定の個体を対象として、その正当性を認証する認証装置であって、前記個体から、当該個体を特徴づける第１対象情報を取得する対象情報取得手段と、前記取得された対象情報に基づいて、前記個体の正当性を認証する対象情報認証手段と、前記正当性が認証された個体が存在する位置を表わす位置情報を取得して前記対象情報に対応づける位置情報付加手段とを備える。

また、上記目的を達成するために、本発明に係る認証装置は、電波時計システムから前記個体が存在する時刻を表わす時間情報を取得して付加することを特徴とする。

【０００８】

さらに、上記目的を達成するために、本発明に係る認証システムは、特定の個人及び当該個人が所持する特定の物品のうち、少なくとも一つの個体を対象として、当該個体の正当性と当該個体が実存することを認証するための認証サーバと、当該認証サーバにネットワークを介して接続されている認証用端末とからなる認証システムであって、前記認証用端末は、前記個体から、当該個体を特徴づける対象情報を取得する対象情報取得手段と、前記個体が存在する位置を表わす位置情報を取得する位置情報取得手段と、取得された前記対象情報及び前記位置情報を前記認証サーバに送信する送信手段とを備え、前記認証サーバは、前記認証用端末から対象情報及び位置情報とを受信する受信手段と、前記受信された対象情報に基づいて、前記個体の正当性を認証する対象情報認証手段と、前記受信された位置情報に基づいて、前記個体が存在する位置を認証する位置情報認証手段と、前記個体の正当性が認証され、前記位置情報が認証された場合に、前記個体が実存すると認証する実存認証手段とを備える。

【０００９】

なお、上記目的を達成するために、本発明は、上記認証装置の特徴的な手段をステップとする認証方法として実現したり、それらのステップをパソコン等のコンピュータに実行させるプログラムとして実現することもできる。そして、そのようなプログラムをＣＤ－ＲＯＭ等の記録媒体やインターネット等の伝送媒体を介して流通させることもできる。

【００１０】

【発明の実施の形態】

以下、本発明に係る実施の形態について、図面を参照しながら説明する。

（実施の形態１）

図１は、本実施の形態の一例であり、宅配会社の配達人が物品を配達する際に、本実施の形態における認証装置２００を用いて種々の認証を行なう様子を示した図である。図１には、宅配会社１００の配達人１１０が、配達先宅１３０において、受取人１２０に物品１５０を渡す様子が示されている。この際、配達人１１０は、認証装置２００を用いて、配達人、物品、配達先及び配達時刻等の認証を行なう。

ここで、「認証」とは、行為や文書等が正当な行為者や正当な手続き等によって行なわれたことを証明することをいい、例えば、特定の個人であること、実在すること、正当な授受が行なわれたこと、内容の改竄がないことなどを証明する場合が該当する。

【００１１】

具体的には、配達人１１０が物品１５０を受取人１２０に渡す際に、認証装置２００を用いて配達人１１０の指紋を採取し、この指紋が認証装置２００に予め登録されている配達人１１０の指紋と一致した場合に「配達人が認証された」こととする。さらに、物品１５０のバーコード１５１を読み取り、予めこのバーコードに対応付けられて登録されている住所１５２と、この場所でＧＰＳ衛星１４０を介して取得した位置情報とが一致した場合に「物品及び配達先が認証された」こととする。さらにまた、予め上記バーコードに対応付けられて登録されている配達時間帯の中に、配達時に取得（例えば、内蔵されている時計や電波時計等から取得）した時刻が入っている場合に「配達時刻が認証された」こととする。

【００１２】

図２は、上記図１における認証装置２００の外観図である。認証装置２００は、物品１５０の配達時に配達人１１０の操作により、「配達人」、「物品」、「配達先」及び「配達時刻」について認証を行なうスタンドアロン型の端末であり、表示パネル２２０、赤外線ポート２３０、指紋読取センサ２４０、キーボード

２５０、メモリスロット２６０、バーコードリーダ２７０及びアンテナ２８０等が筐体２１０に格納されている。

表示パネル２２０は、例えば、液晶パネルであり、キーボード２５０を介してオペレータから受け付けた操作入力の内容や上記の認証結果の表示等を行なう。図２には、種々の認証結果や手続きの状況等の表示例が示されている（２２１～２２４）。

【００１３】

赤外線ポート２３０は、ＩｒＤＡの規格等に基づいて、赤外線を用いることによりＰＣ(Personal Computer)など、他の情報端末とのデータ通信を可能とするための入出力ポートである。

指紋読取センサ２４０は、指紋を読み取るための静電容量方式又は光学式等のセンサであり、この上に置かれた指の指紋を取り込む。

【００１４】

メモリスロット２６０は、例えば、ＳＤメモリカード等の小型記憶媒体に対する読み出し／書き込みを行なうためのインターフェース装置である。例えば、この小型記憶媒体には、予め配達前に宅配会社５００において、配達すべき物品のＩＤコード毎に、受取人の氏名及びその住所１５２、配達予定の配達人のＩＤコード及び配達予定時間帯等が予め記憶されている。なお、配達人のＩＤコードとその配達人の指紋データは、別途内蔵するメモリ（図示せず）に格納され、宅配会社１００の管理者等によって登録／更新等が行なわれ、安全が確保されているものとする。

【００１５】

バーコードリーダ２７０は、上記の配達される物品１５０に添付されているバーコード１５１を読み取るための（例えば、ＯＣＲ型又はＣＣＤ型等の）装置である。

アンテナ２８０は、例えば、ＰＨＳや携帯電話の基地局（図示せず）又はＧＰＳ衛星１４０等から送信される位置情報や時間情報等を受信するためのアンテナである。

【００１６】

図３は、上記図２の認証装置２００の機能構成を示すブロック図である。図３に示されるように、認証装置２００は、入力部１０、表示部２０、演算制御部３０、対象情報処理部４０、送受信制御部５０、時間情報認証部６０、位置情報処理部７０、映像生成部８０及び記憶部９０等を備えている。

入力部１０は、本装置２００に必要なデータの取得及びオペレータからの操作入力を受け付ける部分であり、対象情報取得部１１及びユーザ入力部１２から構成されている。

対象情報取得部１１は、上記図２における指紋読取センサ２４０やバーコードリーダ２７０を含み、認証の対象とする物（例えば、個人や物品など）から、それらを個別に識別することが可能な情報（以下、「対象情報」という。）を取得し、演算制御部３０に送信する。

【００１７】

ここで、個人を認証する場合の対象情報としては、オペレータから入力されたＩＤコードやパスワード、指紋読取センサ２４０等から入力される指紋データ、声紋データ、顔の特徴を表わした画像データ、虹彩データ、ＤＮＡデータなどがある。なお、これらの対象情報のうち、１つの対象情報によって認証を行なうこととしてもよいし、２以上の対象情報を組み合わせて、より高精度で認証を行なうこととしてもよい。一方、物品を認証する場合の対象情報としては、物品のＩＤコード（バーコードを含む。）や物品の特徴を表わした画像データなどがある。

【００１８】

ユーザ入力部１２は、上記図２におけるキーボード２５０に対応する部分であり、必要に応じてオペレータからＩＤコードやパスワード等のキーボード入力を受け付ける。

表示部２０は、上記図２における表示パネル２２０を含み、ユーザ入力部１２を介して入力された内容や認証結果の表示等を行なう。

【００１９】

演算制御部３０は、例えば、ＲＯＭやＲＡＭ等を備えるマイクロコンピュータなどであり、認証装置２００全体の制御を行なう。さらに、演算制御部３０は、

対象情報取得部１１から対象情報を受信して対象情報処理部４０に送信する。この場合、演算制御部３０は、必要に応じて受信した対象情報をデータベースとして記憶部９０に記憶する。さらにまた、演算制御部３０は、内部に計時が可能なクロックを備えており、時間情報取得部６１から要求があった場合は、その時刻を表わす時間情報を返す。なお、演算制御部３０は、いわゆる電波時計を内蔵し、これに基づいて時間情報を送信することとしてもよい。

対象情報処理部４０は、演算制御部３０を介して受信した対象情報について、認証処理を行なったり、対象情報ＤＢ４２に記憶されている対象情報の更新を行なう機能を有しており、対象情報認証部４１、対象情報ＤＢ４２及び対象情報更新部４３から構成される。

【００２０】

対象情報認証部４１は、演算制御部３０から受信した対象情報と対象情報ＤＢ４２に予め記憶されている情報とを照合し、一致／不一致等の判定を行ない、その結果を演算制御部３０に通知する。例えば、対象情報取得部１１において入力された配達人の指紋データと予め対象情報ＤＢ４２に記憶されている指紋データとを照合し、一致するものがある場合は、その指紋データに対応する「配達人ＩＤ」を演算制御部３０に通知し、一致しない場合は「該当者なし」を通知する。対象情報取得部１１から、配達人の指紋データの以外のデータ、例えば、ＩＤコードやパスワード、声紋データ、顔の特徴に関するデータ、虹彩データ及びＤＮＡデータ等を入力し、これに基づいて予め登録されているデータとの照合を行ない、その結果を演算制御部３０に通知することとしてもよい。

【００２１】

対象情報ＤＢ４２は、例えば、ＲＡＭやハードディスク等であり、個人や物品を識別するためのＩＤコードやパスワード、指紋データ、声紋データ、顔の特徴に関するデータ、虹彩データ及びＤＮＡデータ等を記憶する。上記データの登録／更新等は、特定の者のみが実施することとし、安全が確保されているものとする。

対象情報ＤＢ更新部４３は、演算制御部３０の指示により、対象情報ＤＢ４２に記憶されている対象情報の登録／更新等を行なう。

【００２２】

送受信制御部５０は、現在位置や現在時刻の特定に必要な位置情報や時間情報を取得するために、ＧＰＳ衛星、ＰＨＳ、携帯電話等との通信を行なう機能を有しており、ＧＰＳデータ受信部５１、位置情報受信部５２及びデータ送信部５３を備える。

ＧＰＳデータ受信部５１は、ＧＰＳ衛星５５０から位置情報や時間情報を受信する。位置情報受信部５２は、ＰＨＳや携帯電話の基地局からの位置情報や、ビーコンからの位置情報などを受信する。データ送信部５３は、上記図２における赤外線ポート２３０、及びＰＨＳや携帯電話における送信制御回路等に対応する部分であり、演算制御部３０から受信した認証結果等のデータをＰＣや他の携帯情報端末等に送信する。

【００２３】

時間情報認証部６０は、演算制御部３０から受信した時間情報と記憶部９０に予め記憶されている情報（例えば、上記の配達時間帯）とを照合し、その結果を演算制御部３０に通知する。例えば、ＧＰＳデータ受信部５１を介して取得された時間情報と予め記憶部９０に記憶されている配達時間帯とを照合し、この配達時間帯に時間情報が示す時刻が含まれている場合は、「時間内配達」を演算制御部３０に通知し、上記時刻が含まれていない場合は「時間外配達」を通知する。

【００２４】

位置情報処理部７０は、送受信制御部５０及び演算制御部３０を介して受信した位置情報と予め位置情報ＤＢ７２に記憶されているデータを照合することにより位置の認証を行なう機能を有しており、位置情報生成認証部７１、位置情報ＤＢ７２及び位置情報ＤＢ更新部７３から構成されている。

位置情報生成認証部７１は、演算制御部３０を介して受信した位置情報を、予め位置情報ＤＢ７２に記憶されている位置情報に合わせて変換（例えば、経度／緯度を実際の住所に変換）し、変換後の位置情報と予め位置情報ＤＢに記憶されている位置情報と照合し、一致／不一致を判定する。判定結果は、演算制御部３０に通知する。

【００２５】

位置情報ＤＢ７２は、例えば、ハードディスクやＲＡＭ等であり、上記位置情報の変換を行なうためのデータが記憶されている。例えば、緯度／経度で表現されている位置情報を住所（○○県△△市・・等）に変換する（又はその逆の変換を行なう）ためのデータベースである。

位置情報ＤＢ更新部７３は、演算制御部３０の指示に従って、位置情報ＤＢ７２の内容の更新等を行なう。

映像生成部８０は、オペレータによって取得された映像（例えば、配達対象の物品の外観やＩＤコードなど）の映像データや、バーコードの読み取り結果等を記憶する。

【００２６】

記憶部９０は、上記図２におけるメモリスロット２６０や小型記憶媒体、ＲＡＭ等であり、演算制御部３０の指示により、上記のように、配達前に登録される配達すべき物品のＩＤコード毎の受取人の氏名及びその住所、予定配達人のＩＤコード及び配達予定時間帯や、認証結果として登録される物品ＩＤコード毎の配達人ＩＤ、配達位置、配達日時などが記憶される。なお、上記小型記憶媒体は、ＳＤカードやマルチメディアカードなどに代表される任意のメモリカードの他、フレキシブルディスク等であってもよい。

【００２７】

図４～図６は、上記図３における対象情報ＤＢ４２又は記憶部９０に格納されるデータの構成例である。

図４は、対象情報ＤＢ４２に格納される配達人指紋データ等の構成例である。図４に示されるように、配達人指紋データ４０３は、配達人ＩＤ４０１及び配達人氏名４０２に対応付けられて、予め（配達開始前に）対象情報ＤＢ４２に格納される。なお、この指紋データの登録／更新等については、一部の担当者のみが行ない、配達人は、登録／変更等を行なうことができないこととする。

【００２８】

図５は、記憶部９０に格納される配達用データテーブルの構成例である。ここで、「配達用データテーブル」とは、未配達の物品に関する情報をまとめたテーブルであり、当日、配達が開始される前に登録される。図５に示されるように、

配達用データテーブル５００には、物品ＩＤ５０１毎に、受取人氏名５０２、受取人住所５０３及び配達予定時間帯５０４が、予め（配達開始前に）記憶部９０に格納される。なお、上記配達予定時間帯５０５の欄には、年月日を合わせて登録することとしてもよい。また、この配達用データの登録／更新等については、担当者が登録／変更等を行なうこととする。

【００２９】

図６は、記憶部９０に登録される配達完了時における認証結果データテーブルの構成例である。ここで、「認証結果データテーブル」とは、物品の配達に際して、種々の認証に必要な情報や認証結果をまとめたテーブルであり、配達完了時に格納される。図６に示されるように、認証結果データテーブル６００としては、物品ＩＤ６０１毎に、配達人ＩＤ６０２、配達位置６０３、配達日時５０４及び受取人指紋データ６０５が、配達完了時に記憶部９０に格納される。ここで、配達人ＩＤ６０２は、配達時に配達人の指紋データと予め登録されている指紋データとが一致した場合に、対応する配達人ＩＤが記載される。また、経度と緯度で示される配達位置６０３及び配達日時６０４は、バーコードリーダ２７０によって物品ＩＤが読み込まれた場合に、自動的にＧＰＳ衛星等から取得して格納される。受取人指紋データ６０５は、物品の配達を完了した確認として、受取人から取得する。

【００３０】

次に、上記の宅配会社１００の配達人１１０が、物品１５０を配達する場合において、認証装置２００を用いて種々の認証を行なう場合の認証装置２００の処理の流れについて説明する。

【００３１】

図７は、本認証装置２００の処理の様子を示したフローチャートである。

最初に、演算制御部３０は、表示部２０に、「配達人の指紋を入力して下さい。」等の表示を行ない（Ｓ７０１）、配達人からの指紋の入力を待つ（Ｓ７０２）。

指紋が入力されると、演算制御部３０は、対象情報ＤＢ４２を参照し、当該配達人が正当な配達人であるか否かを判別するように、対象情報認証部４１に指示す

る。この場合、正当な配達人であると判別されると、当該配達人は「認証された」こととなる（Ｓ７０３）。

【００３２】

次に、演算制御部３０は、表示部２０に、「物品のバーコードを入力して下さい。」等の表示を行ない（Ｓ７０４）、物品に添付されているバーコードの入力を待つ（Ｓ７０５）。バーコードが入力されると、演算制御部３０は、対象情報ＤＢ４２を参照し、当該物品が配達予定の物品であるか否かを判別するように、対象情報認証部４１に指示する。配達予定の物品であると判別されると、当該物品は「認証された」こととなる（Ｓ７０６）。

【００３３】

さらに、演算制御部３０は、表示部２０に、「受取人の指紋を入力して下さい。」等の表示を行ない（Ｓ７０７）、受取人からの指紋の入力を待つ（Ｓ７０８）。指紋が入力されると、演算制御部３０は、送受信制御部５０に、位置情報及び時間情報を取得するように指示する（Ｓ７０９）。位置情報及び時間情報が取得されると、演算制御部３０は、配達位置、配達時刻が正当か否かを判別するように、位置情報処理部７０及び時間情報認証部６２に指示する（Ｓ７１０）。

さらに、演算制御部３０は、上記の認証結果を表示部２０に送信する（Ｓ７１１）。

【００３４】

以上のように、本実施の形態の認証装置２００によれば、予め登録され、その安全性が確保されているデータと動的に取得したデータとを照合してその正当性を判別するので、「特定の位置」に「特定の個体（人や物）」が「存在すること」や「正当な授受が行なわれたこと」等を認証することが可能となる。

なお、上記実施の形態では、「配達人の指紋」、「物品ＩＤ」、「受取人の指紋」の順で認証を行なったが、認証順序は任意である。また、個人を認証するための対象情報として指紋データを用いる例を示したが、指紋データに限るものではなく、上記のように、声紋データ、顔の特徴を示す画像データ、虹彩データ等を用いることとしてもよい。

【００３５】

また、上記実施の形態の対象情報認証部４１及び位置情報生成認証部７１における認証方法は、一般の認証手法を用いることができる。例えば、所定の認証機関が作成した認証実行コードを用いることもできる。また、後に述べるサーバから各端末（この場合は各認証装置）の認証用コードを所定の条件に沿って動的に制御し、認証精度を保つ（なりすましなどを防ぐ）ことも可能である。

【００３６】

さらに、上記実施の形態において、物品１５０の認証に用いる対象情報は、バーコード１５１に限定するものではなく、物品を認証する任意の情報（外観の映像データ等）であってもよい。このとき、タグが物品Ｓに添付されていることを映像生成部８０で画像として確認することもできる。これによって物品Ｓからタグが外れていないことなどを確認することが可能となる。

なお、物品Ｓの画像から直接、物品Ｓを認証することもできる。物品ＳがＢ氏のもとに届けられた際に、認証装置１によって、その場所と物品Ｓを認証することで確かにその場所に物品Ｓが届けられたことが証明される。

【００３７】

例えば、前述のＡ氏がＢ氏への重要な物品Ｓの配達を配達会社Ｄ社に依頼した場合を考えると、Ｂ氏の認証と物品Ｓの認証を行なうことで、Ｄ社はＡ氏に対して「Ｂ氏に物品Ｓが渡ったこと」を証明することができる。Ｄ社の虚偽申告（実際には物品Ｓを渡していないにもかかわらず「渡した」と申告すること）や、なりすまし（Ｂ氏以外の人物がＢ氏に代わって物品Ｓを受け取ること）を防ぐことができ、Ｄ社としても、確実に荷物の配達を終えたことを証明できる。これは、配達証明郵便や、その他任意の「特定の人物」と「特定の物品」の認証によって意味をなす事象に応用できる。

【００３８】

（実施の形態２）

上記の実施の形態１においては、スタンドアロンで使用する認証装置２００について説明したが、本実施の形態では、ネットワークを介して構成される認証システム３００について説明する。この認証システム３００は、認証装置２０１から指紋データや位置情報等の認証に必要なデータを受信した認証サーバ３１０が

、これらのデータに基づいて種々の認証（例えば、出張として訪問した「訪問者」とその「訪問先」、「訪問時刻」等の認証等）を行なうシステムである。

なお、以下においては、上記実施の形態１と異なる構成について重点的に説明し、共通する構成については同一の符号を付して、その説明は省略することとする。

【００３９】

図８は、本実施の形態における認証システム３００のシステム構成図である。図８に示されるように、本システム３００は、インターネット等のネットワーク３２０を介して認証装置２０１から認証サーバ３１０に対象情報を送信し、認証サーバ３１０が、受信した対象情報に基づいて認証を行なうものである。

認証装置２０１は、認証サーバ３１０に対象情報を送信するための端末であり、上記実施の形態１の認証装置２００と同じ機能を有しているが、認証装置２００における対象情報処理部４０、時間情報認証部６０及び位置情報処理部７０を有していなくてもよい。

【００４０】

一方、認証サーバ３１０は、認証装置２０１から対象情報を受信し、この情対象報に基づいて、種々の認証を行なうサーバ（例えば、通信機能及びサーバ機能を有するパーソナルコンピュータ等）であり、上記認証装置２００における演算制御部３０、対象情報処理部４０、時間情報認証部６０及び位置情報処理部７０を有する（図示せず）。

【００４１】

図９は、認証システム３００による管理対象の一例である出張の様子を示した図であり、出張における予定ルートと訪問予定時刻（図９では（）内に示されている。）とを表わした図である。図９に示されるように、社員９０１は、１０時に会社９１０を訪問し、その後、１３時に会社９２０、１５時に会社９３０、１６時に会社９４０を順次訪問することとする。その際、社員９０１は、それぞれの訪問先に到着時に、指紋データ、位置情報等を認証サーバ３１０に送信する。これにより、営業所９００における管理者９０２は、「訪問者」、「訪問先」及び「訪問時刻」を認証する。

【００４２】

図１０は、上記認証サーバ３１０に格納される、社員９０１の出帳予定を表わすデータを格納したテーブル（以下、「出張予定テーブル」という。）の構成例である。図１０に示されるように、この出張予定テーブル１０００は、訪問先会社名１００１毎に、その会社の所在地１００２、訪問予定者ＩＤ１００３及び訪問予定日時１００４を表わすデータが格納される。この出張予定テーブルは、社員９０１の出張前に、認証サーバ３１０の記憶部９０に格納される。

【００４３】

図１１は、上記認証サーバ３１０に格納される、社員９０１の出張結果を表わすデータを格納するテーブル（以下、「出張結果テーブル」という。）の構成例である。図１１に示されるように、この出張結果テーブル１１００は、訪問先会社名１１０１毎に、訪問位置１１０２、訪問者ＩＤ１１０３、訪問日時１１０４を表わすデータ及び訪問者の指紋データ１１０５が登録される。この出張結果テーブルの各データは、社員９０１（又は認証用端末２０１のオペレータ）が出張先の会社に到着後（認証装置２０１から対象情報を受信し、その認証後）に、認証サーバ３１０の記憶部９０に格納される。なお、図１１において“－”は、その会社には未到着のため、未設定のデータであることを表わしている。

【００４４】

図１２は、社員９０１の出張時の認証サーバ３１０と認証装置２０１間における通信シーケンス図である。

まず、社員９０１の出張前に、出張予定テーブル１０００に、必要なデータが登録される（Ｓ１２０１）。次に、社員９０１は、出張先の会社に到着すると到着処理として、自分の「指紋データ」、取得した「位置情報」及び「時刻情報」を認証サーバ３１０に送信する（Ｓ１２０２、Ｓ１２０３）。これにより、認証サーバ３１０は、受信した上記の情報に基づいて、認証処理として「訪問者」、「訪問先」及び「訪問時刻」の認証を行ない、出張結果テーブル１１００に所定のデータを登録する（Ｓ１２０４）。

以下、予定に従って順次会社に到着する度に、上記の処理が繰り返される（Ｓ１２０５）。

【００４５】

図１３は、上記図１２の認証用端末２０１における到着処理の様子を示すフローチャートである。

最初に、認証用端末２０１の演算制御部３０は、表示部２０に、「出張者の指紋を入力して下さい。」等の表示を行ない（Ｓ１３０１）、オペレータからの指紋の入力を待つ（Ｓ１３０２）。指紋が入力されると、演算制御部３０は、指紋データを生成する（Ｓ１３０３）。

次に、演算制御部３０は、送受信制御部５０に、位置情報及び時間情報を取得するように指示する（Ｓ１３０４）。位置情報及び時間情報が取得されると、演算制御部３０は、上記の指紋データ、位置情報及び時間情報を認証サーバ３１０に送信する（Ｓ１３０５）。

【００４６】

図１４は、上記図１２における認証処理１２０４の様子を示すフローチャートである。

最初に、認証サーバ３１０の演算制御部３０は、認証用端末２０１から出張人の指紋データ、位置情報及び時間情報を受信すると(Ｓ１４０１)、予め対象情報ＤＢ４２に記憶されている訪問者の指紋データ、記憶部９０に記憶されている所在地１００２及び訪問予定日時１００４に基づいて、それぞれ訪問者、訪問先及び訪問時刻を認証する(Ｓ１４０２～Ｓ１４０４)。なお、上記Ｓ１４０２～Ｓ１４０４の各処理の認証順序は図１４の限りではなく任意である。

また、本認証システム３００は、上記の出張管理に限らず、著作物における著作者等の認証や、施錠管理における担当者等を認証する場合に応用可能である。

【００４７】

図１５は、本認証システム３００を用いて、写真の著作物における著作者と撮影場所等を認証する場合の認証サーバ３１０と認証用端末２０１間における通信シーケンス図である。

最初に、認証用端末２０１は、撮影者の操作によって写真のデータを取り込むと(Ｓ１５０１)、図１３と同様の手順で取得された（“訪問者”を“撮影者”にして適用。）、写真データ、指紋データ、撮影した場所の位置情報及び撮影した

時刻の時間情報を認証サーバ３１０に送信する(Ｓ１５０２、Ｓ１５０３)。

【００４８】

次に、認証サーバ３１０の演算制御部３０は、認証用端末２０１から写真データ、指紋データ、位置情報等を受信すると、予め登録しておいた撮影者の指紋データに基づいて撮影者を認証する(Ｓ１５０４)。さらに、認証サーバ３１０の演算制御部３０は、予め登録しておいた撮影予定場所を表わす情報に基づいて、撮影場所（撮影者の現在位置）を認証する(Ｓ１５０５)。

なお、上記の撮影対象から上記バーコードのように対象物を識別し得る情報を取得することができる場合は、併せてこの情報を認証サーバ３１０に送信して、より高い精度で認証を行なうこととしてもよい。

【００４９】

図１６は、本認証システム３００を用いて、「ある施設の施錠管理者が、その施設内に作業者がいない場合に施錠を行なう場合」の、作業者とその場所等を認証する場合の認証サーバ３１０と認証用端末２０１間における通信シーケンス図である。この場合、作業者は、認証用端末２０１を所持しており、認証サーバ３１０は、管理センター（図示せず）内に設置されているものとする。さらに、施錠管理者自身が管理センター内にいる場合にのみ、その施設に対して施錠することが可能であるとする。

最初に、作業員が施設から退場すると、認証用端末２０１は、作業員から指紋の入力を受け付け(Ｓ１６０１)、位置情報及び時間情報を取得する(Ｓ１６０２)。さらに、認証用端末２０１は、取得した指紋データ及び位置情報等を認証サーバ３１０に送信する(Ｓ１６０３)。

【００５０】

次に、管理センター内の認証サーバ３１０は、受信した作業員の指紋データ及び位置情報等に基づいて、作業員が施設内に居ないことを認証し(Ｓ１６０４、Ｓ１６０５)する。さらに、認証サーバ３１０は、管理者からの指紋データと位置情報及び時間情報を取得し、管理者が管理センター内に居ることを認証する(Ｓ１６０６、Ｓ１６０７)。以上の認証により、施設内に作業員が居ないことを確認すると（Ｓ１６０８）、認証サーバ３１０は、施設の施錠を行なうことが可

能となる(Ｓ１６０９)。

なお、上記のシステムは、作業員が複数の場合であっても、同様の認証を各作業員について繰り返すことによって、同様の施錠管理が可能である。

【００５１】

以上のように、本実施の形態に係る認証システムを用いることにより、ネットワークを介して認証用端末から認証サーバに対象物とその位置情報等を送信し、認証サーバで認証を行なうので、遠隔地において、より確度の高いなセキュリティシステムを構築することが可能となる。

なお、認証装置の内部に認証処理を高速化させるために、上記の対象情報ＤＢや位置情報ＤＢ以外に、ＬＵＴ：Logical Unit Table）を用いることとしてもよい。これを用いることにより、認証に必要なデータの入力を削減させることが可能となる。

【００５２】

なお、複数の認証を重畳して行なうことにより、認証精度を高めることもできる。例えば、認証装置の誤認証率が、それぞれ１０００分の１であった場合、２台の認証装置を用いて認証することにより、１００万分の１に誤認証率を下げることができる。

なお、上記の複数台の認証装置と同様に、一つの認証対象物、人に対して、複数の認証用データを用いることで認証精度を向上することもできる。

【００５３】

さらには、２つの認証がともに承認された場合に限り、認証を有効にすることにより、物品受け渡しなどの際に勘合符がわりとして使用する（物品の受け渡しを行なう）こともできる。複数の認証用データを用いることによる機能は上記に限定されず、任意の機能実現に複数の認証用データを用いることができる。

なお、特定の認証装置の認証機能そのものを他の認証装置が認証することやサーバが認証することもできる。

【００５４】

なお、認証装置は認証手段として秘密鍵や公開鍵、一方向性関数の逆演算の困難性に基づく暗号などの暗号技術や汗等によるＤＮＡ認証を用いてもよい。

なお、認証方法が複数ある場合は、通信環境や装置の性能等などに応じて認証サーバが動的に選択し、その認証方法を認証用端末に通知することとしてもよい。

さらに、オペレータのパスワード等が第三者等に漏れてしまった場合に、例えば「パスワードが漏れている可能性があります。」など、オペレータに警告を提示するように構成してもよい。また、当該装置の使用を停止するように制御してもよい。

【００５５】

【発明の効果】

以上のように、本発明に係る認証装置により、

（１）「特定の物品」が「特定の位置」存在すること、又は「特定の個人」と「特定の物品」とを認証したい状況（特定の住所に対する配達の認証、物品受け渡しの認証など）

（２）「特定の位置」に「特定の人物」が存在することを認証したい状況（営業マンの巡回管理、オリエンテーリング状況管理など）

（３）個体（例えば、個人や物品等）の「特定の行動や移動」を認証したい状況（出張管理、産業廃棄物の廃棄管理、撮影データや録音データ等の著作証明など）

（４）一つ以上の「個体とその位置の認証」により、新たな２次的効果を得たい状況（特定の施設に対するリモート施錠管理など）

といった各状況に対して、有効に機能する認証装置を提供することが可能となる。

【図面の簡単な説明】

【図１】

実施の形態１に係る、宅配会社の配達人が物品を配達する際における認証装置を用いて種々の認証を行なう様子を示した図である。

【図２】

図１における認証装置の外観図である。

【図３】

認証装置の機能構成を示すブロック図である。

【図４】

対象情報ＤＢに格納される配達人指紋データ等の構成例である。

【図５】

記憶部に格納される配達用データテーブルの構成例である。

【図６】

記憶部に登録される配達完了時における認証結果データテーブルの構成例である。

【図７】

認証装置の処理の様子を示したフローチャートである。

【図８】

実施の形態２における認証システムのシステム構成図である。

【図９】

認証システムによる管理対象の一例である出張の様子を示した図である。

【図１０】

認証サーバに格納される、社員の出帳予定を表わす出張予定テーブルの構成例である。

【図１１】

認証サーバに格納される、社員の出張結果を表わすデータを格納する出張結果テーブルの構成例である。

【図１２】

社員の出張時の認証サーバと認証装置間における通信シーケンス図である。

【図１３】

図１２の認証用端末における到着処理の様子を示すフローチャートである。

【図１４】

図１２における認証処理の様子を示すフローチャートである。

【図１５】

認証システムを用いて、写真の著作物における著作者と撮影場所等を認証する場合の認証サーバと認証用端末間における通信シーケンス図である。

【図１６】

認証システムを用いて、「ある施設の施錠管理者が、その施設内に作業者がいない場合に施錠を行なう場合」の、作業者とその場所等を認証する場合の認証サーバと認証用端末間における通信シーケンス図である。

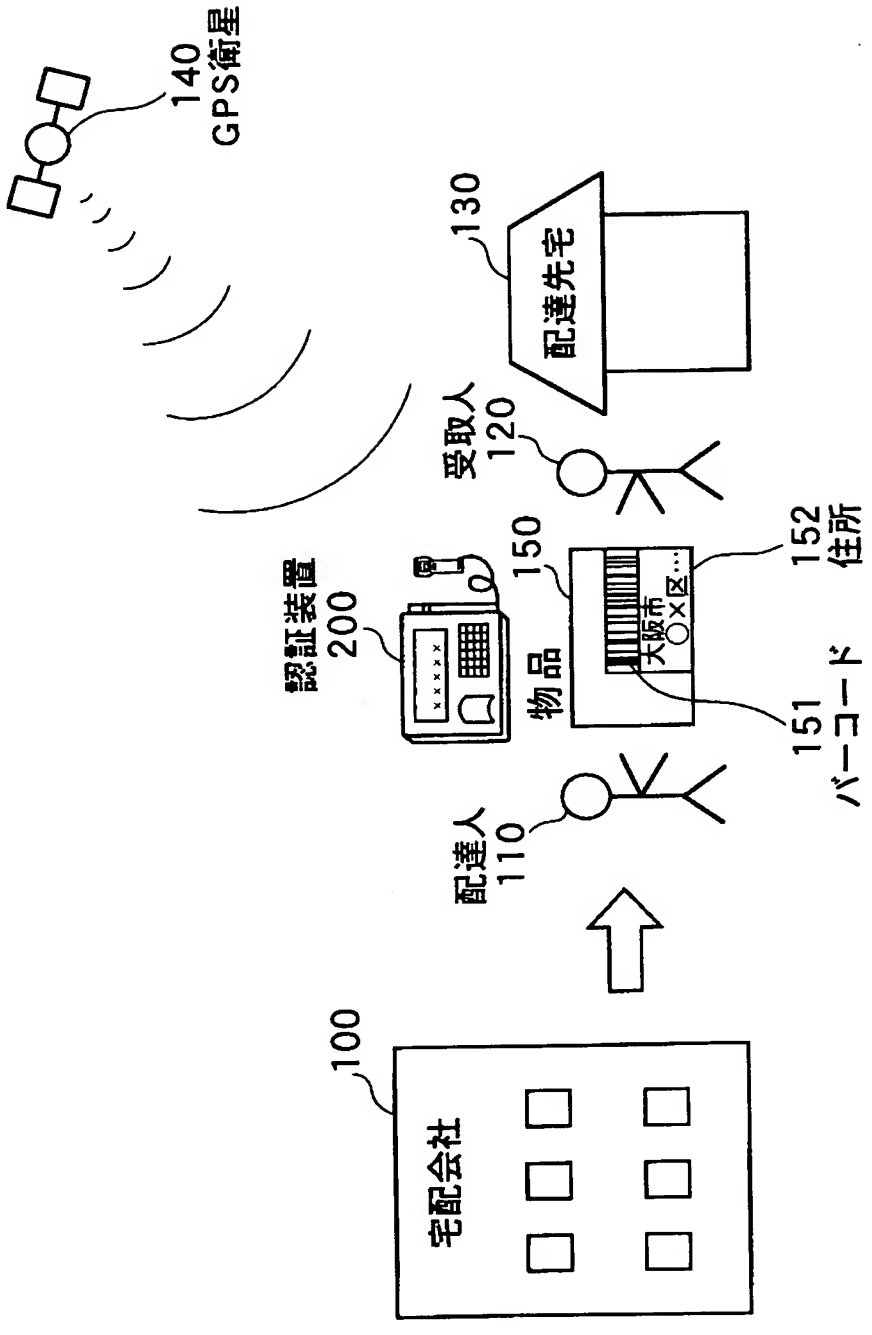
【符号の説明】

１０	入力部
１１	対象情報取得部
１２	ユーザ入力部
２０	表示部
３０	演算制御部
４０	対象情報処理部
４１	対象情報認証部
４２	対象情報ＤＢ
４３	対象情報ＤＢ更新部
５０	送受信制御部
５１	ＧＰＳデータ受信部
５２	位置情報受信部
５３	データ送信部
６０	時間情報認証部
７０	位置情報処理部
７１	位置情報生成認証部
７２	位置情報ＤＢ
７３	位置情報ＤＢ更新部
８０	映像生成部
９０	記憶部
２００	認証装置
２０１	認証用端末
２１０	筐体
２２０	表示パネル

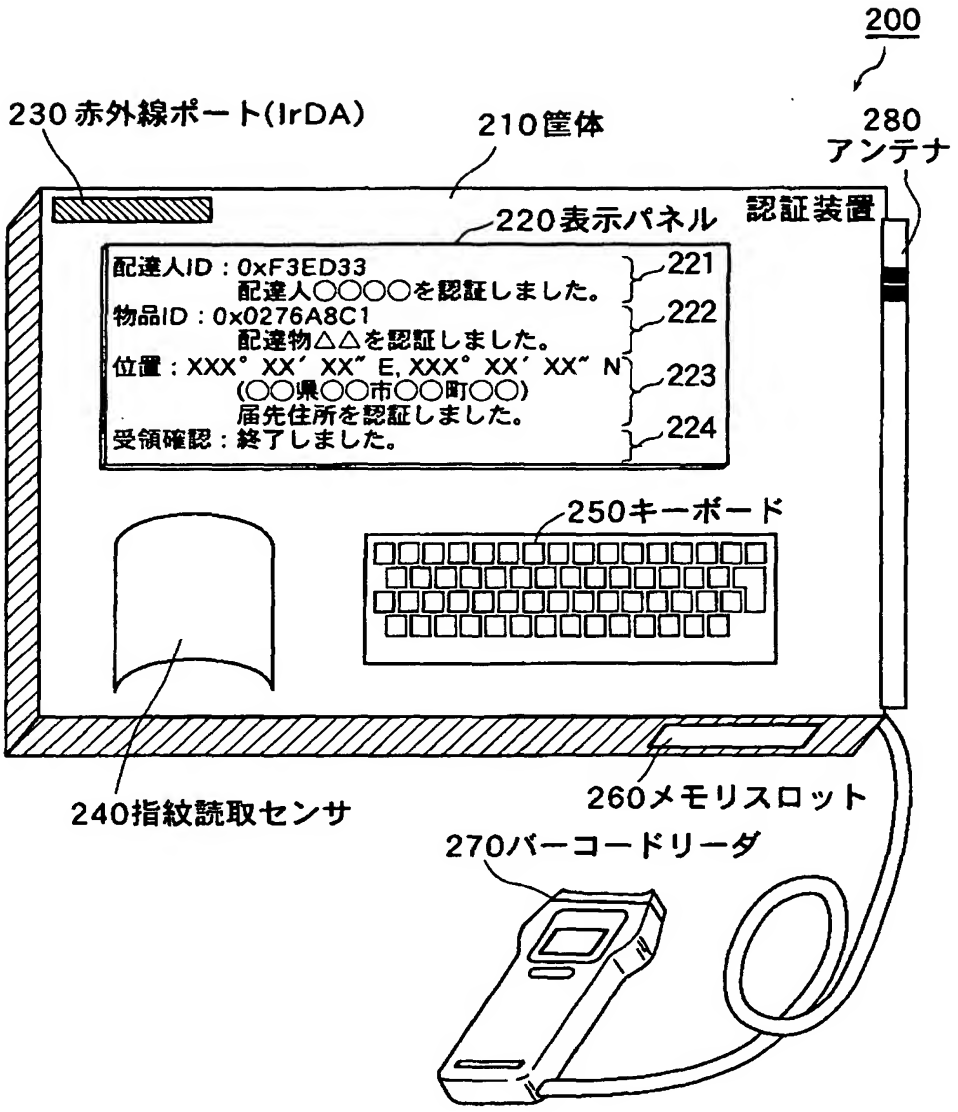
２３０　赤外線ポート
２４０　指紋読取センサ
２５０　キーボード
２６０　メモリスロット
２７０　バーコードリーダ
２８０　アンテナ
３００　認証システム
３１０　認証サーバ
３２０　ネットワーク

【書類名】　　図面

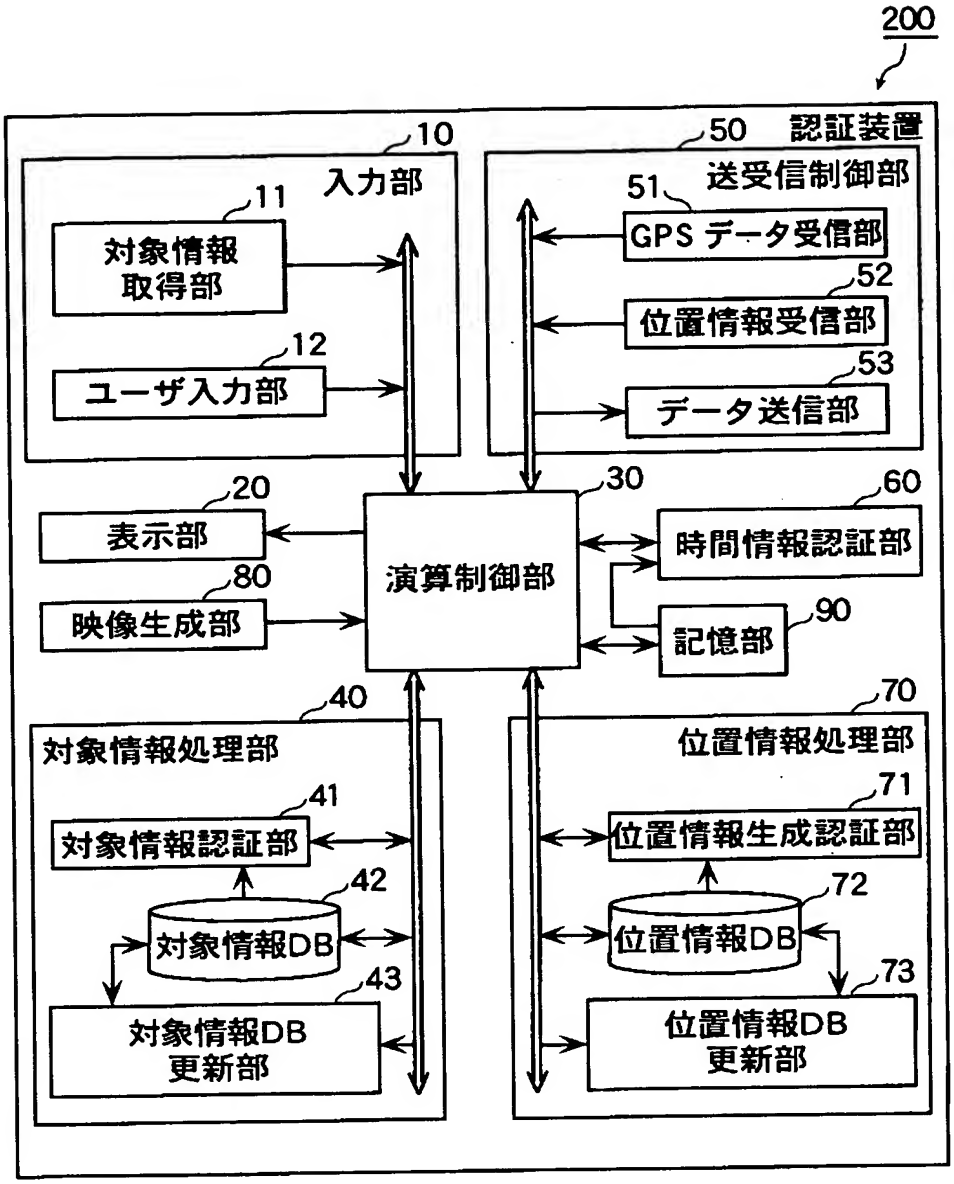
【図１】


140
GPS衛星
130
配達先宅
受取人
120
認証装置
200
150
物品
152
住所
大阪市
○×区…
151
バーコード
配達人
110
100
宅配会社

【図２】


200
230 赤外線ポート(IrDA)
210筐体
280
アンテナ
220表示パネル
認証装置
配達人ID：0xF3ED33
配達人○○○○を認証しました。
221
物品ID：0x0276A8C1
配達物△△を認証しました。
222
位置：XXX° XX′ XX″ E, XXX° XX′ XX″ N
(○○県○○市○○町○○)
届先住所を認証しました。
223
受領確認：終了しました。
224
250キーボード
240指紋読取センサ
260メモリスロット
270バーコードリーダ

【図３】

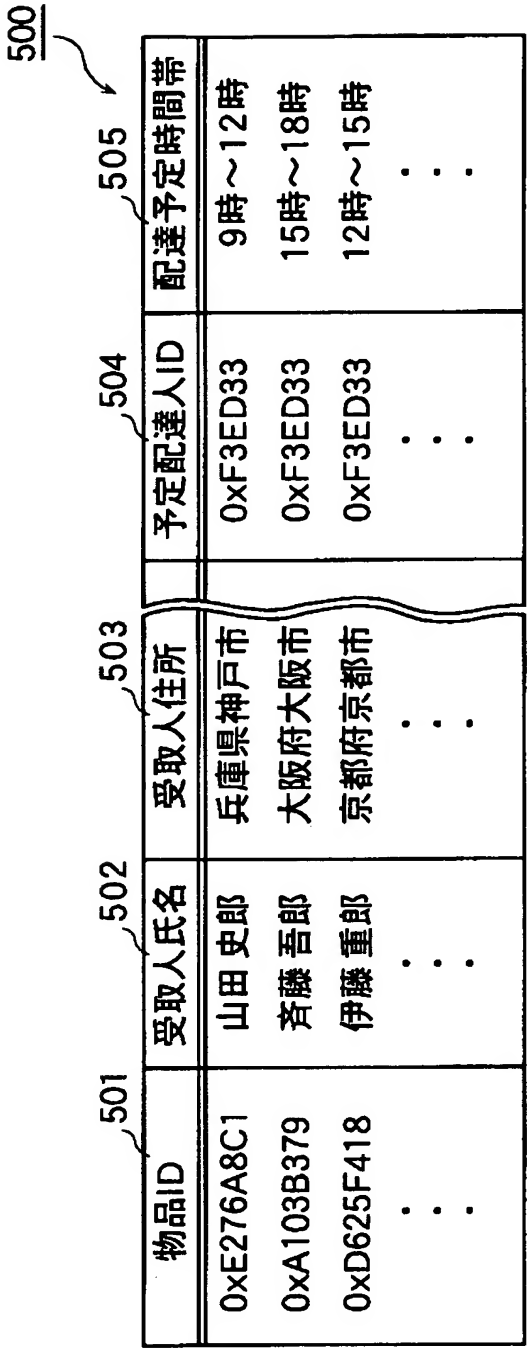

200
認証装置
10
入力部
11
対象情報
取得部
12
ユーザ入力部
50
送受信制御部
51
GPS データ受信部
52
位置情報受信部
53
データ送信部
20
表示部
80
映像生成部
30
演算制御部
60
時間情報認証部
90
記憶部
40
対象情報処理部
41
対象情報認証部
42
対象情報DB
43
対象情報DB
更新部
70
位置情報処理部
71
位置情報生成認証部
72
位置情報DB
73
位置情報DB
更新部

【図４】

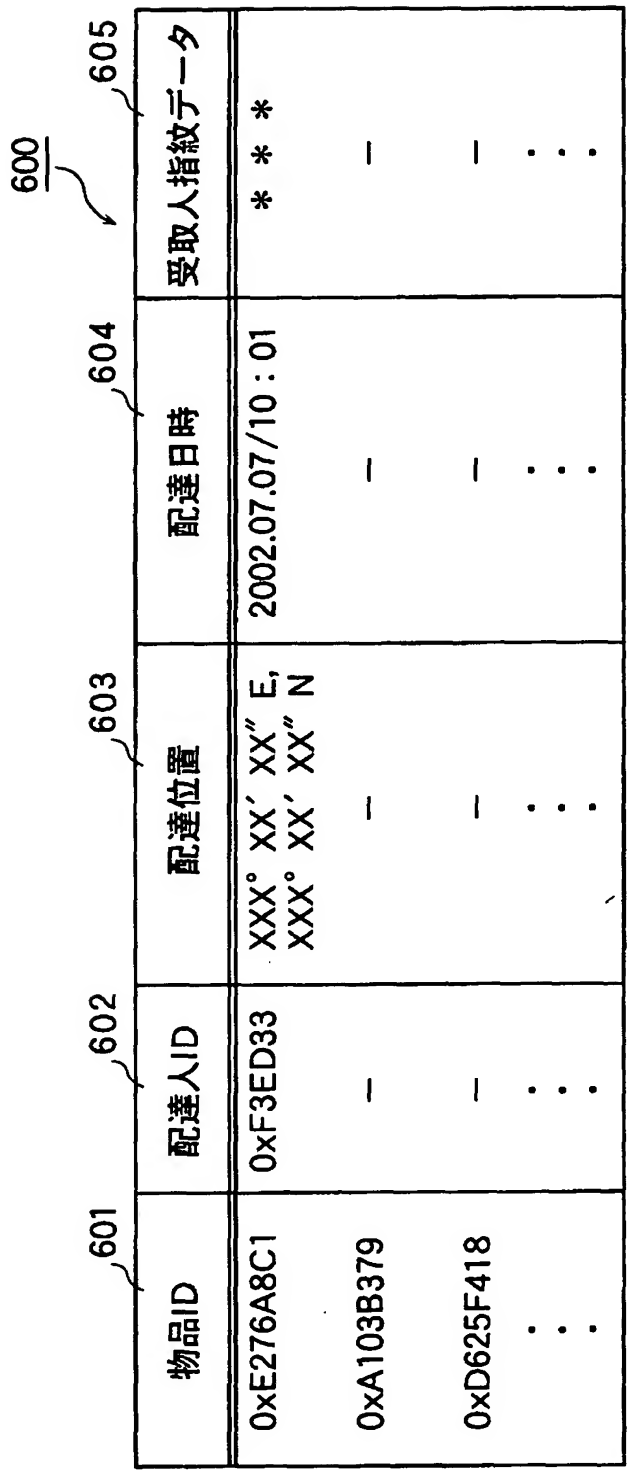
400

401 配達人ID	402 配達人氏名	403 配達人指紋データ
0xF3ED33	佐藤 一子	＊ ＊ ＊
0xM4AH75	鈴木 次郎	＊ ＊ ＊
0xM8CB18	高橋 三郎	＊ ＊ ＊
・	・	・
・	・	・
・	・	・

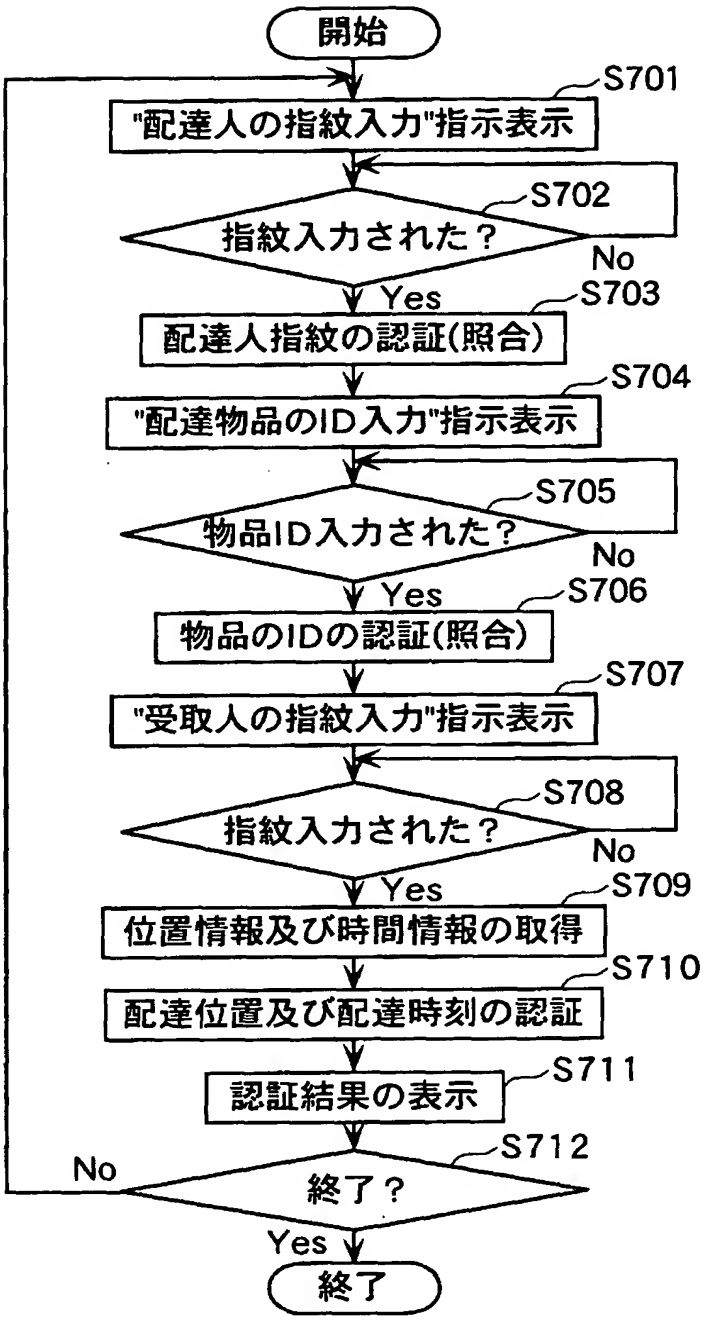
【図５】


500
501
502
503
504
505
物品ID
受取人氏名
受取人住所
予定配達人ID
配達予定時間帯
0xE276A8C1
0xA103B379
0xD625F418
山田 史郎
斉藤 吾郎
伊藤 重郎
兵庫県神戸市
大阪府大阪市
京都府京都市
0xF3ED33
0xF3ED33
0xF3ED33
9時～12時
15時～18時
12時～15時

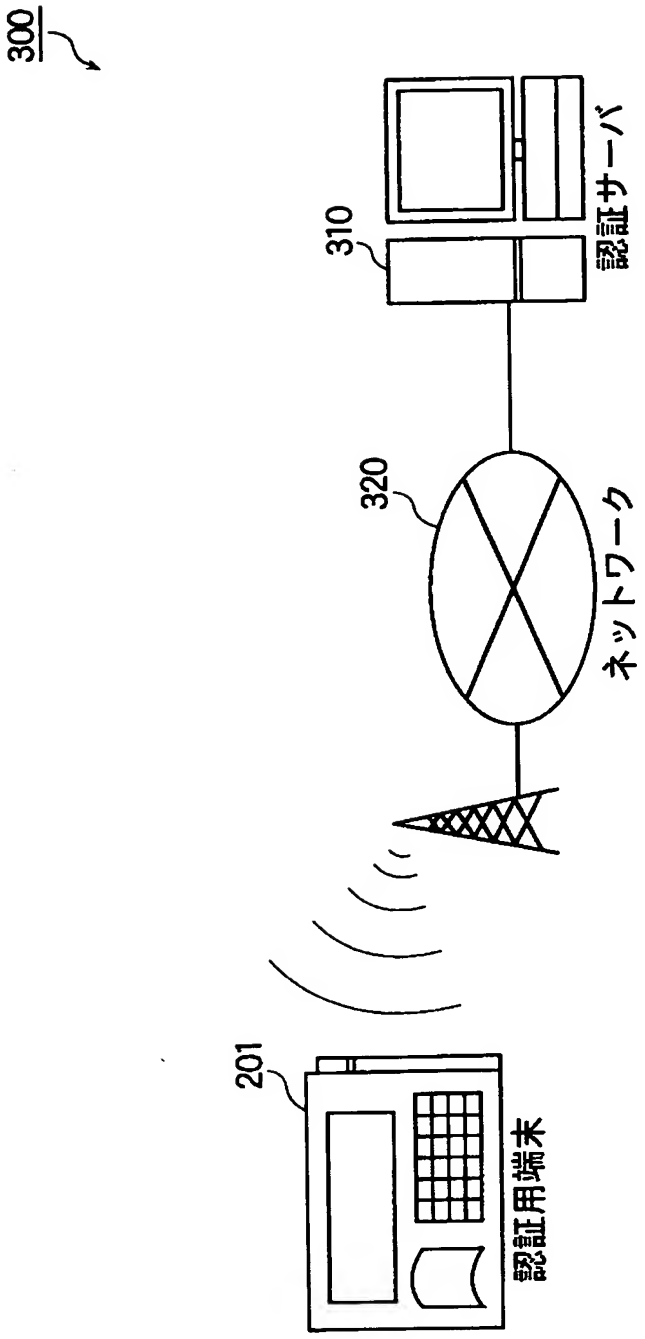
【図６】


600
601
602
603
604
605
物品ID
配達人ID
配達位置
配達日時
受取人指紋データ
0xE276A8C1
0xF3ED33
XXX° XX′ XX″ E,
XXX° XX′ XX″ N
2002.07.07/10：01
＊＊＊
0xA103B379
－
－
－
－
0xD625F418
－
－
－
－
・・・
・・・
・・・
・・・
・・・

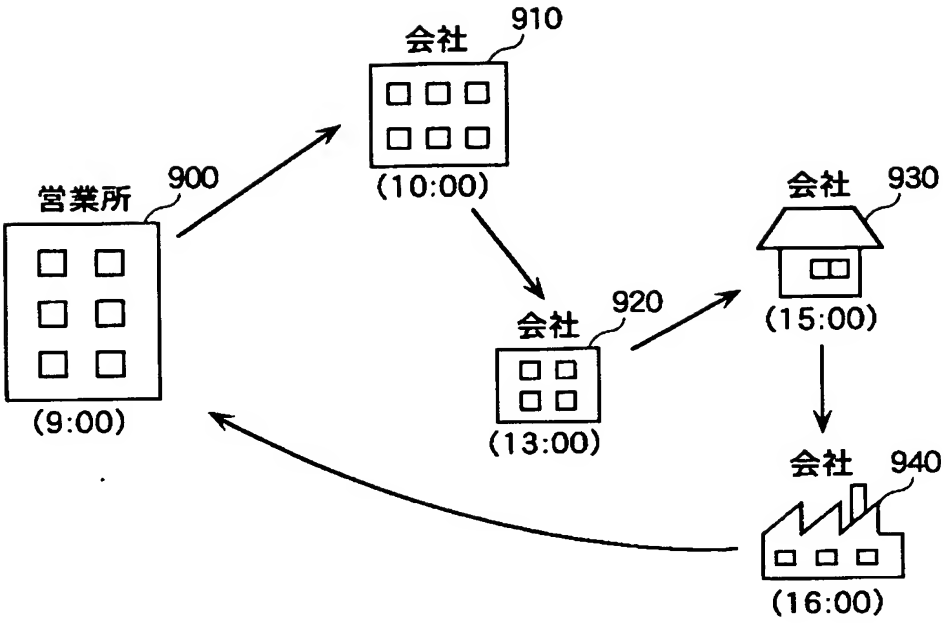
【図７】


開始
S701
"配達人の指紋入力"指示表示
S702
指紋入力された？
No
Yes
S703
配達人指紋の認証(照合)
S704
"配達物品のID入力"指示表示
S705
物品ID入力された？
No
Yes
S706
物品のIDの認証(照合)
S707
"受取人の指紋入力"指示表示
S708
指紋入力された？
No
Yes
S709
位置情報及び時間情報の取得
S710
配達位置及び配達時刻の認証
S711
認証結果の表示
S712
No
終了？
Yes
終了

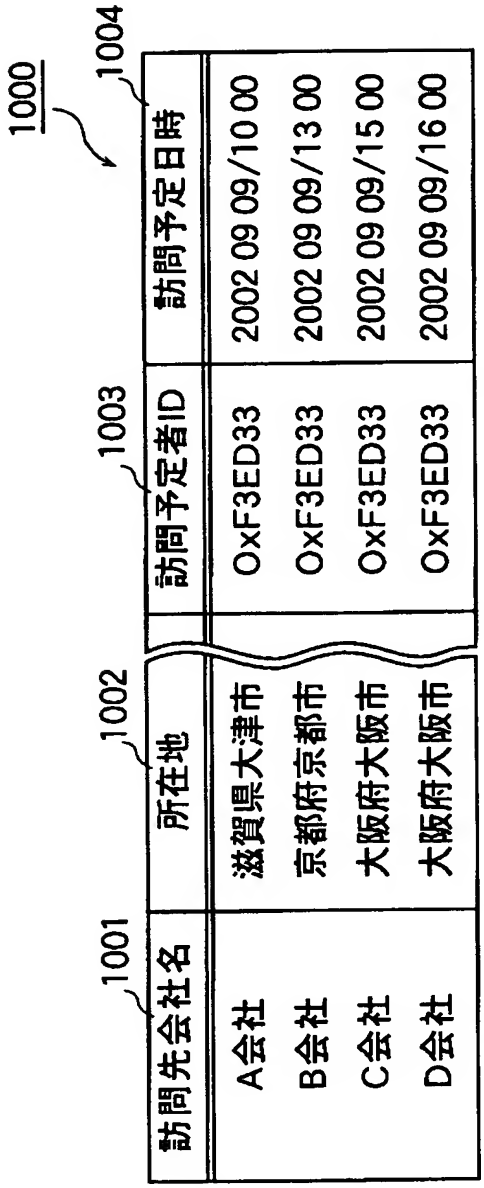
【図８】



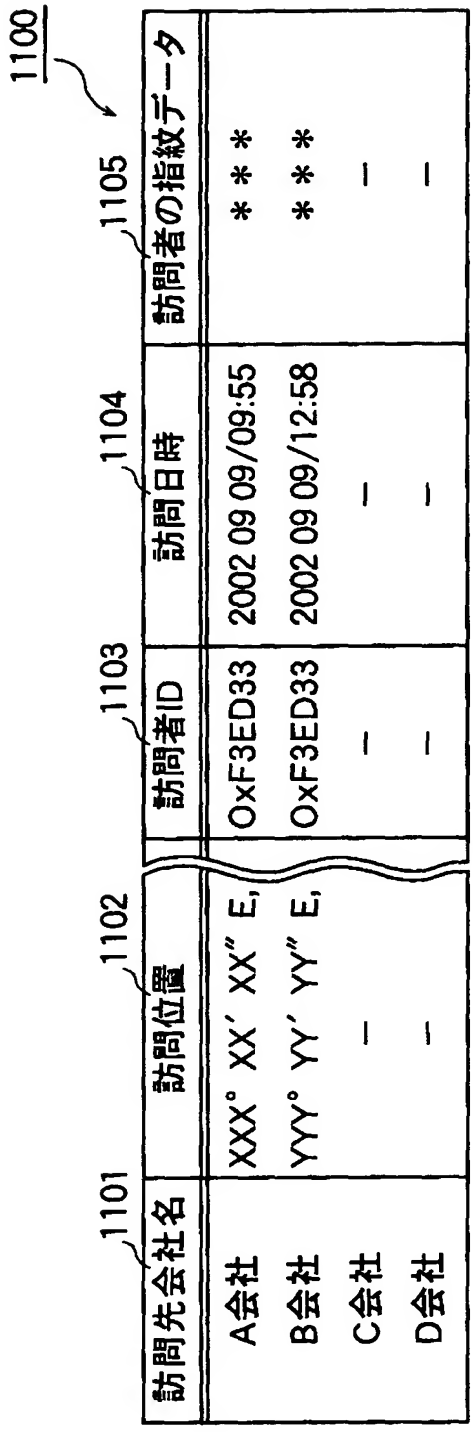
【図９】



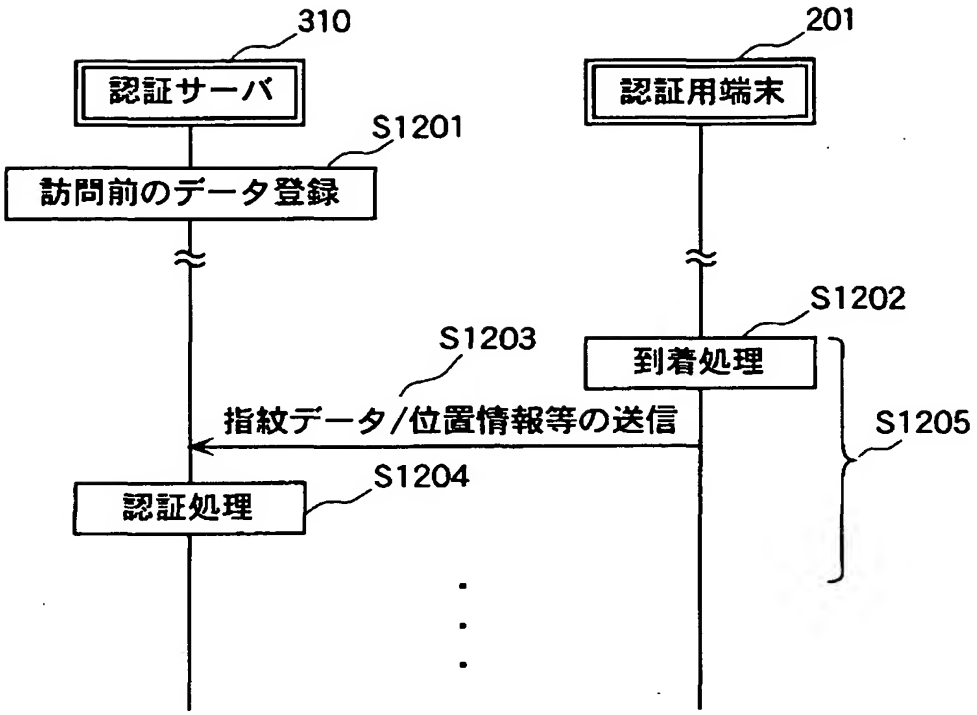
【図１０】


1000
1001
1002
1003
1004
訪問先会社名
所在地
訪問予定者ID
訪問予定日時
A会社
滋賀県大津市
OxF3ED33
2002 09 09/10 00
B会社
京都府京都市
OxF3ED33
2002 09 09/13 00
C会社
大阪府大阪市
OxF3ED33
2002 09 09/15 00
D会社
大阪府大阪市
OxF3ED33
2002 09 09/16 00

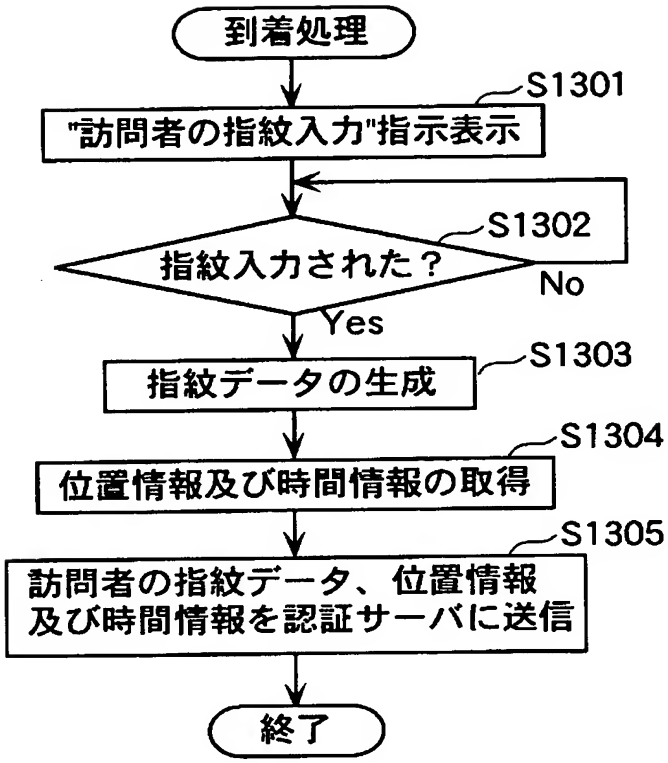
【図１１】


1100
1101
訪問先会社名
1102
訪問位置
1103
訪問者ID
1104
訪問日時
1105
訪問者の指紋データ
A会社
XXX° XX′ XX″ E,
OxF3ED33
2002 09 09/09:55
＊＊＊
B会社
YYY° YY′ YY″ E,
OxF3ED33
2002 09 09/12:58
＊＊＊
C会社
－
－
－
－
D会社
－
－
－
－

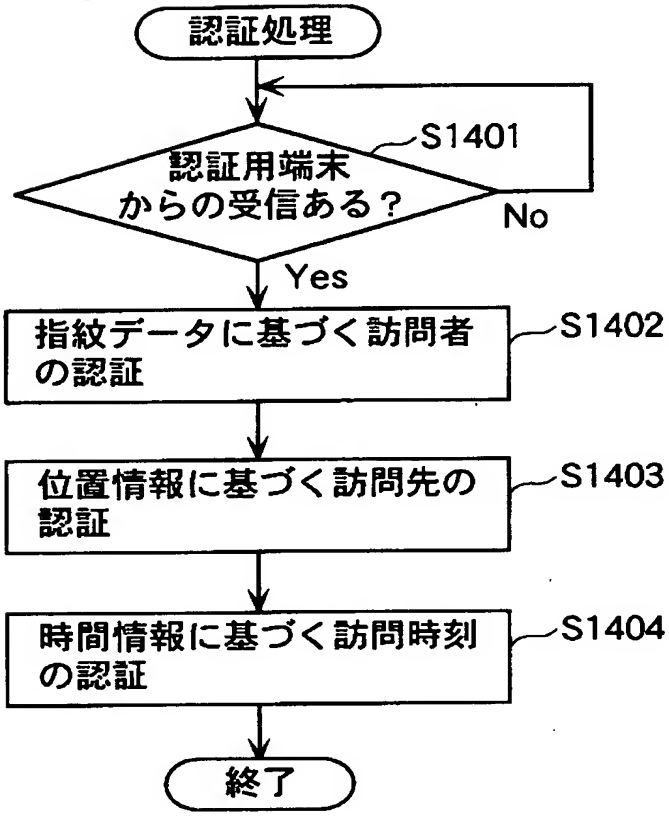
【図１２】


310
認証サーバ
201
認証用端末
S1201
訪問前のデータ登録
S1202
S1203
到着処理
指紋データ/位置情報等の送信
S1205
S1204
認証処理

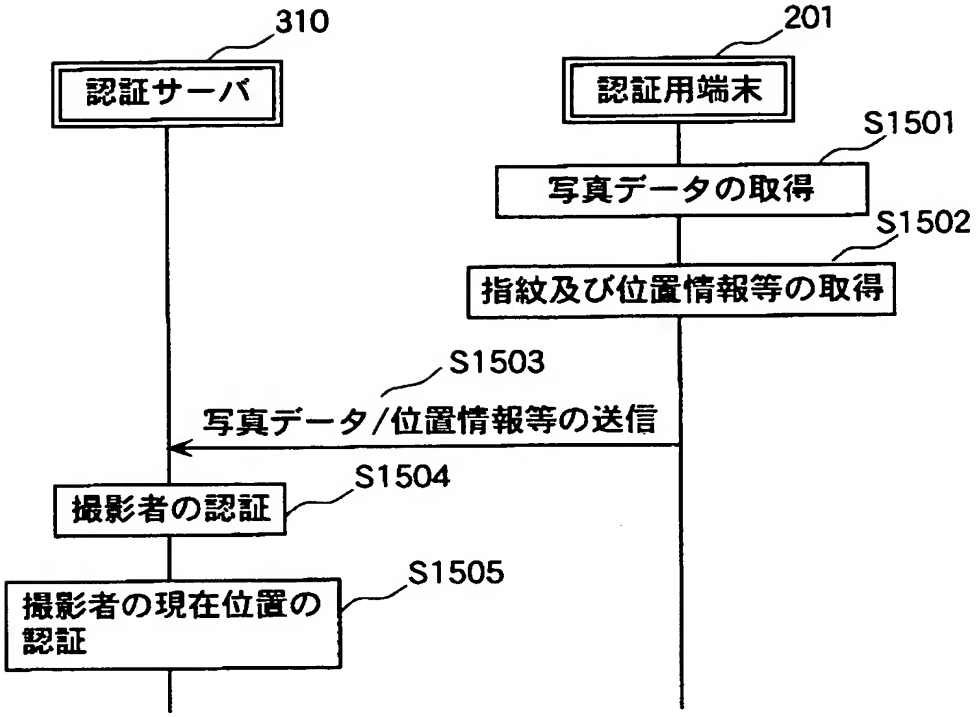
【図１３】


到着処理
S1301
"訪問者の指紋入力"指示表示
S1302
指紋入力された？
No
Yes
S1303
指紋データの生成
S1304
位置情報及び時間情報の取得
S1305
訪問者の指紋データ、位置情報
及び時間情報を認証サーバに送信
終了

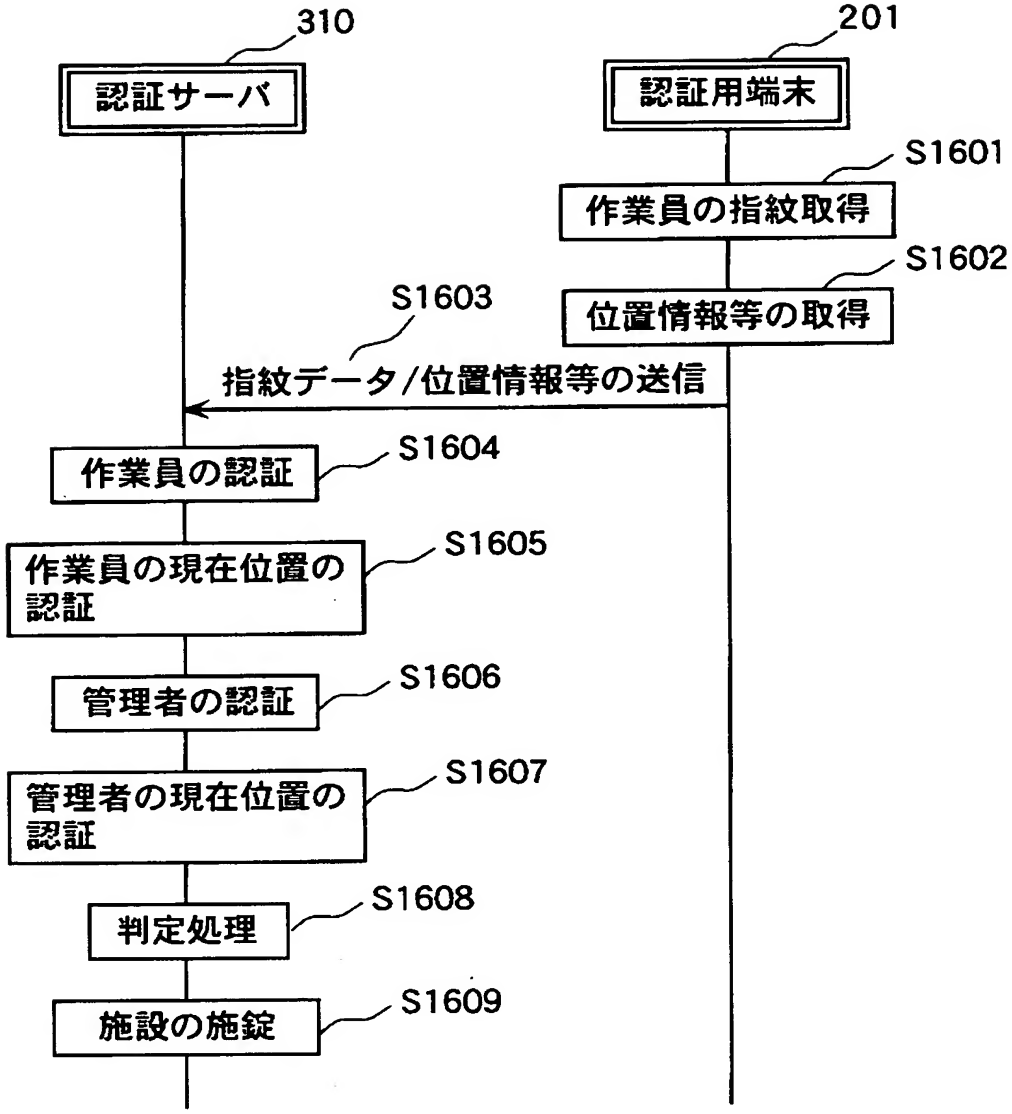
【図１４】


認証処理
S1401
認証用端末からの受信ある？
No
Yes
指紋データに基づく訪問者の認証
S1402
位置情報に基づく訪問先の認証
S1403
時間情報に基づく訪問時刻の認証
S1404
終了

【図１５】


310
認証サーバ
201
認証用端末
S1501
写真データの取得
S1502
指紋及び位置情報等の取得
S1503
写真データ/位置情報等の送信
S1504
撮影者の認証
S1505
撮影者の現在位置の認証

【図１６】


310
認証サーバ
201
認証用端末
S1601
作業員の指紋取得
S1602
位置情報等の取得
S1603
指紋データ/位置情報等の送信
S1604
作業員の認証
S1605
作業員の現在位置の認証
S1606
管理者の認証
S1607
管理者の現在位置の認証
S1608
判定処理
S1609
施設の施錠

【書類名】　　要約書

【要約】

【課題】　「特定の位置」に「特定の個人（又は物品）」が存在することを認証し得る認証装置を提供する。

【解決手段】　対象情報取得部１１やユーザ入力部１２により、対象物の認証に必要な情報（対象情報）を取得する。取得された対象情報は、演算制御部３０を介して認証対象情報処理部４０に入力され、対象情報認証部４１によって個人、物品等が認証される。この認証の際、対象情報ＤＢ４２を利用する。また、ＧＰＳデータ受信部５１や位置情報受信部５２により、現在位置の特定に必要な位置情報を取得する。この位置情報は、ＧＰＳ衛星、携帯電話やＰＨＳの基地局等から取得する。位置情報認証部７１は、取得された位置情報と予め記憶部９０に記憶されている情報に基づいて、位置の認証を行なう。この認証の際、位置情報ＤＢ７２を利用する。

【選択図】　図３

認定・付加情報

特許出願の番号	特願２００２－２２６５３２
受付番号	５０２０１１５１５２９
書類名	特許願
担当官	小野寺　光子　　１７２１
作成日	平成１４年　８月　５日

＜認定情報・付加情報＞

【提出日】　平成14年 8月 2日

次頁無

出 願 人 履 歴 情 報

識別番号　〔０００００５８２１〕

１．変更年月日　１９９０年　８月２８日
［変更理由］　新規登録
住　所　大阪府門真市大字門真１００６番地
氏　名　松下電器産業株式会社